

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-287476
(43)Date of publication of application : 14.10.2004

(51)Int.CI. G06F 12/00

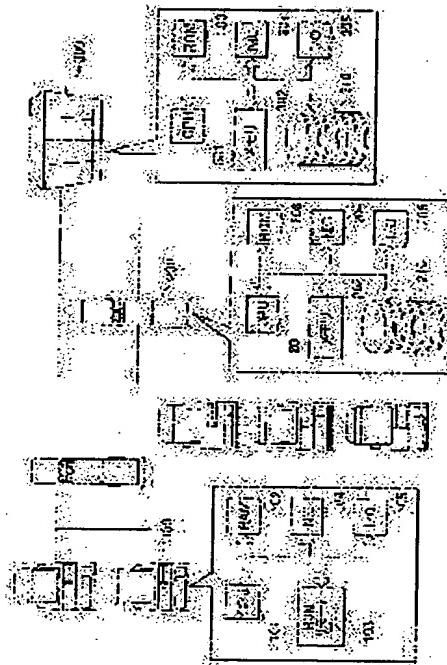
(21)Application number : 2003-075181 (71)Applicant : HITACHI LTD
(22)Date of filing : 19.03.2003 (72)Inventor : KIMURA SHINJI
OSHIMA SATOSHI
HASHIMOTO TAKASHI

(54) CACHE CONTROL FOR NODE DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve security of data against the theft of a node device and unauthorized access in a computer system comprising a client, the node device and a storage device.

SOLUTION: In the computer system capable of transferring data through the node device between the client and storage device, cache in the node device is controlled in the following method. In the first control, the attribute of cache propriety is given on data stored in the storage device, and the node device carries out relay to the client without performing cache on cache-disabled data. In the second control, the node device enciphers data in caching to a disk. In the third control, the cache-disabled data are directly transmitted and received without passing through the node device. With this control, cache to the node device can be limited to ensure security.



LEGAL STATUS

[Date of request for examination] 04.10.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特願2004-287476

(P2004-287476A)

(43) 公開日 平成16年10月14日(2004.10.14)

(51) Int. Cl.⁷

G06F 12/00

F 1

G06F 12/00 546K

G06F 12/00 537Z

テーマコード(参考)

5B082

審査請求 未請求 請求項の数 28 O L (全 25 頁)

(21) 出願番号

特願2003-75181 (P2003-75181)

(22) 出願日

平成15年3月19日 (2003.3.19)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(74) 代理人 110000028

特許業務法人明成国際特許事務所

(72) 発明者 木村 信二

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所

内

(72) 発明者 大島 誉

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所

内

最終頁に続く

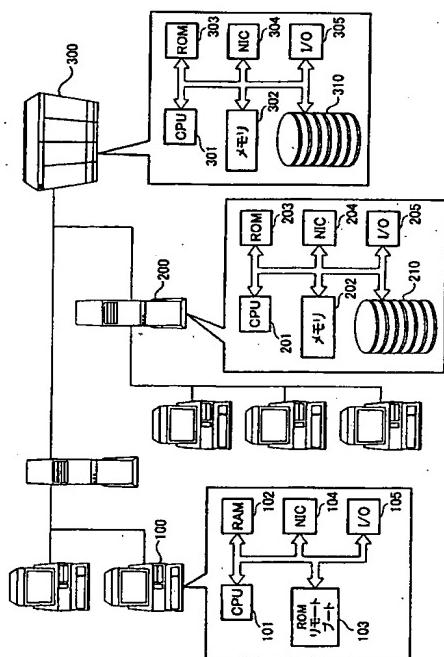
(54) 【発明の名称】 ノード装置におけるキャッシング制御

(57) 【要約】

【課題】クライアント、ノード装置、ストレージ装置からなる計算機システムにおいて、ノード装置の盗難、不正アクセスに対するデータのセキュリティを向上する。

【解決手段】クライアントおよびストレージ装置間で、ノード装置を介してデータを授受可能な計算機システムにおいて、ノード装置におけるキャッシングを次の方法で制御する。第1の制御では、ストレージ装置に格納されているデータについてキャッシング可否の属性を付与しており、ノード装置は、キャッシング不可とされているデータについては、キャッシングを行わずにクライアントへの中継を行う。第2の制御では、ノード装置は、ディスクへのキャッシング時にデータの暗号化を行う。第3の制御では、キャッシング不可のデータについては、ノード装置を介さずに直接送受信する。これらの制御により、ノード装置へのキャッシングを制限でき、セキュリティを確保することができる。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ストレージ装置、キャッシュ用のディスク装置を備えるノード装置、およびクライアントが接続された計算機システムにおいて、前記ディスク装置へのキャッシングを制御するキャッシング制御方法であって、

前記ストレージ装置またはクライアントにおいて、

前記ノード装置によって中継されるデータについて、前記ディスク装置へのキャッシングの可否を表す属性情報を前記ノード装置に対して出力するステップを実行し、
前記ノード装置において、

前記属性情報に基づいて、前記中継するデータの前記ディスク装置へのキャッシング可否を 10
判断するステップと、

キャッシング否と判断されたデータについては、前記ディスク装置へのキャッシングを行わずに中継するステップとを実行するキャッシング制御方法。

【請求項 2】

ストレージ装置、キャッシュ用のディスク装置を備えるノード装置、およびクライアントが接続された計算機システムにおいて、前記ディスク装置へのキャッシングを制御するキャッシング制御方法であって、

前記ノード装置において、

中継すべきデータを、前記ストレージ装置またはクライアントから入力するステップと、
前記中継するデータを暗号化して前記ディスク装置に書き込むステップと、

前記ディスク装置に保持されているデータの読み出コマンドに応じて、該ディスク装置から
読み出したデータを復号して前記ストレージ装置またはクライアントに出力するステップとを実行するキャッシング制御方法。 20

【請求項 3】

ストレージ装置、キャッシュ用のディスク装置を備えるノード装置、およびクライアントが接続された計算機システムにおいて、前記ディスク装置へのキャッシングを制御するキャッシング制御方法であって、

前記ノード装置において、

前記ストレージ装置またはクライアント装置から受信したデータを、所定のタイミングで
前記ディスク装置にキャッシングするステップを実行し、

前記ストレージ装置またはクライアントの一方において、

提供するデータについて、所定の条件に基づいて、前記ディスク装置へのキャッシングの可否を判断するステップと、

キャッシング可と判断されたデータについては、前記ノード装置に送信するステップと、
キャッシング否と判断されたデータについては、前記ノード装置を介さずに前記ストレージ
装置またはクライアントの他方に直接データを送信するステップとを実行するキャッシング制御方法。 30

【請求項 4】

キャッシング用のディスク装置を備え、ストレージ装置とクライアントとの間で、データの授受を中継するノード装置であって、

前記中継するデータについて、前記ディスク装置へのキャッシングの可否を表す属性情報を
入力する属性情報入力部と、

該属性情報に基づいて、前記中継するデータの前記ディスク装置へのキャッシング可否を判断する判断部と、

キャッシング否と判断されたデータについては、前記ディスク装置へのキャッシングを行わずに中継するキャッシング制御部とを備えるノード装置。

【請求項 5】

請求項 4 記載のノード装置であって、

前記ディスク装置の他に、キャッシング用の揮発性メモリを有し、

前記キャッシング制御部は、

10

20

30

40

50

前記キャッシュ可否に関わらず前記データを前記揮発性メモリにキャッシュするメモリ制御部と、

前記揮発性メモリから前記ディスク装置への書き込みを行うための所定の条件が成立した場合に、前記キャッシュ否と判断されたデータを除き、該揮発性メモリに保持されたデータを前記ディスク装置に移転する移転制御部とを備えるノード装置。

【請求項 6】

キャッシング用のディスク装置を備え、ストレージ装置とクライアントとの間で、データの授受を中継するノード装置であって、

前記中継するデータを暗号化して前記ディスク装置に書き込む暗号化部と、

前記ディスク装置に保持されているデータの読み出コマンドに応じて、該ディスク装置から読み出したデータを復号して前記ストレージ装置またはクライアントに出力する復号部とを備えるノード装置。 10

【請求項 7】

請求項 6 記載のノード装置であって、

前記中継するデータについて、暗号化の要否を表す属性情報を入力する属性情報入力部と、

該属性情報に基づいて、前記中継するデータの暗号化の要否を判断する判断部と、暗号化要と判断されたデータについては、前記暗号化部および復号部を用いて前記ディスク装置へのキャッシングを行うキャッシング制御部とを備えるノード装置。

【請求項 8】

請求項 6 記載のノード装置であって、

前記ストレージ装置から前記暗号化および復号に使用する鍵データを受信し、揮発性メモリに管理する鍵データ管理部を備えるノード装置。 20

【請求項 9】

請求項 4 ~ 8 いずれか記載のノード装置であって、

前記属性情報は、前記データの中継時に、該データと関連付けて入力されるノード装置。

【請求項 10】

請求項 4 ~ 8 いずれか記載のノード装置であって、

前記属性情報入力部は、前記ストレージ装置におけるデータの格納ブロックと前記属性情報との関係を予め取得し、管理するノード装置。 30

【請求項 11】

請求項 4 ~ 8 いずれか記載のノード装置であって、

前記属性情報は、前記クライアントにおける異常発生を通知する情報であるノード装置。

【請求項 12】

ディスク装置を有するノード装置を介して、クライアントに、データを提供するストレージ装置であって、

前記データについて、前記ディスク装置へのキャッシングの可否、または前記ディスク装置への書き込み時の暗号化の要否を表す属性情報を管理する属性情報管理部と、

前記ノード装置に、該属性情報を通知する属性情報通知部とを備えるストレージ装置。 40

【請求項 13】

請求項 12 記載のストレージ装置であって、

前記属性情報通知部は、前記データの提供時に、該データと関連づけて前記属性情報を通知するストレージ装置。

【請求項 14】

請求項 12 記載のストレージ装置であって、

前記属性情報通知部は、前記データの格納ブロックと前記属性情報との関係をデータの提供に先立って前記ノード装置に通知するストレージ装置。 50

【請求項 15】

請求項 12 記載のストレージ装置であって、

前記ディスクへの書き込み時にデータを暗号化可能な複数のノード装置と接続されており

いずれかの前記ノード装置に対して前記暗号化に用いる鍵データの出力を行うべき所定の条件が満たされたか否かを判断する条件判断部と、
該ノード装置に対して前記鍵データを送信する鍵データ送信部とを備えるストレージ装置。

【請求項 1 6】

ディスク装置を有するノード装置を介してストレージ装置にデータを書き込み可能なクライアントであって、

前記ディスク装置へのキャッシングの禁止、または前記ディスク装置への書き込み時の暗号化を前記ノード装置に要求するための所定の条件が、満たされたか否かを判断する条件判断部と、
10

該条件が満たされた時に、前記ノード装置に対して、前記要求を表す属性情報を出力する禁止通知部と、

該属性情報の出力と併せて、または該属性情報の出力後に、前記データをノード装置に送信するデータ送信部とを備えるクライアント。

【請求項 1 7】

請求項 1 6 記載のクライアントであって、

前記所定の条件は、該クライアントにおけるソフトウェアの動作異常時であるクライアント。

【請求項 1 8】

キャッシング用のディスク装置を備えるノード装置を介して、他の計算機にデータを提供するデータ提供装置であって、

前記提供するデータについて、所定の条件に基づいて、前記ディスク装置へのキャッシングの可否を判断する判断部と、
20

キャッシング可と判断されたデータについては前記ノード装置に送信し、キャッシング否と判断されたデータについては、前記ノード装置を介さずに前記他の計算機に送信する送信制御部とを備えるデータ提供装置。

【請求項 1 9】

請求項 1 8 記載のデータ提供装置であって、

前記提供するデータについて、キャッシングの可否を表す属性情報を予め管理する属性情報管理部を備え、
30

前記判断部は、該属性情報に基づいてキャッシングの可否を判断するデータ提供装置。

【請求項 2 0】

請求項 1 8 記載のデータ提供装置であって、

前記判断部は、該データ提供装置におけるソフトウェアの動作異常時に、キャッシング否と判断するデータ提供装置。

【請求項 2 1】

請求項 1 8 記載のデータ提供装置であって、

前記他の計算機にデータを送信するためのアドレス情報を管理するアドレス管理部を備え
40

前記送信制御部は、前記キャッシング否と判断された場合には、データの送信先を前記ノード装置のアドレスから前記アドレス管理部で管理されているアドレス情報に切り換えるデータ提供装置。

【請求項 2 2】

ストレージ装置と複数のクライアントとの間で、データの授受を中継するノード装置であって、

いずれかの前記クライアントから前記ストレージ装置内のデータの読出コマンドを受け付ける要求受付部と、

該読出コマンドを発信した前記クライアントを特定可能な情報を、該読出コマンドとともに、前記ストレージ装置に送信する要求送信部とを備えるノード装置。
50

【請求項 23】

キャッシング用のディスク装置を備え、ストレージ装置とクライアントとの間で、データの授受を中継するノード装置の動作を制御するコンピュータプログラムであって、前記中継するデータについて、キャッシングの可否を表す属性情報を入力する機能と、該属性情報に基づいて、前記中継するデータのキャッシング可否を判断する機能と、キャッシング否と判断されたデータについては、前記ディスク装置へのキャッシングを行わずに中継する機能とを該ノード装置において実現するためのコンピュータプログラム。

【請求項 24】

キャッシング用のディスク装置を備え、ストレージ装置とクライアントとの間で、データの授受を中継するノード装置の動作を制御するためのコンピュータプログラムであって、前記中継するデータを暗号化して前記ディスク装置に書き込む機能と、該ディスク装置から読み出したデータを復号して前記ストレージ装置またはクライアントに出力する機能とを該ノード装置において実現するためのコンピュータプログラム。 10

【請求項 25】

ディスク装置を有するノード装置を介して、クライアントに、データを提供するストレージ装置の動作を制御するためのコンピュータプログラムであって、前記データについて、前記ディスク装置へのキャッシングの可否、または前記ディスク装置への書き込み時の暗号化の要否を表す属性情報を管理する機能と、前記ノード装置に、該属性情報を通知する機能とを該ストレージ装置において実現するためのコンピュータプログラム。 20

【請求項 26】

ディスク装置を有するノード装置を介してストレージ装置にデータを書き込み可能なクライアントの動作を制御するためのコンピュータプログラムであって、前記ディスク装置へのキャッシングの禁止、または前記ディスク装置への書き込み時の暗号化を、前記ノード装置に要求するための所定の条件が満たされたか否かを判断する機能と、該条件が満たされた時に、前記ノード装置に対して、前記要求を表す属性情報を出力する機能と、該属性情報の出力と併せて、または該属性情報の出力後に、前記データをノード装置に送信する機能とを該クライアントにおいて実現するためのコンピュータプログラム。 30

【請求項 27】

キャッシング用のディスク装置を備えるノード装置を介して、他の計算機にデータを提供するデータ提供装置の動作を制御するコンピュータプログラムであって、前記提供するデータについて、所定の条件に基づいて、前記ディスク装置へのキャッシングの可否を判断する機能と、キャッシング否と判断されたデータについては、前記ノード装置を介さずに前記他の計算機に直接データを送信する機能とを該データ提供装置において実現するためのコンピュータプログラム。

【請求項 28】

ストレージ装置と複数のクライアントとの間で、データの授受を中継するノード装置の動作を制御するコンピュータプログラムであって、いずれかの前記クライアントから前記ストレージ装置内のデータの読出コマンドを受け付ける機能と、該読出コマンドを発信した前記クライアントを特定可能な情報を、該読出コマンドとともに、前記ストレージ装置に送信する機能とを該ノード装置において実現するためのコンピュータプログラム。 40

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、ストレージ装置、クライアント間でデータを中継するノード装置におけるキャ

ツシュの制御に関する。

【0002】

【従来の技術】

企業などでは、複数のクライアントコンピュータ（以下、単にクライアントと称する）をネットワークで接続した大規模な計算機システムが構築されている。このような計算機システムでは、各クライアントで業務を遂行する際に参照する種々のデータやプログラムを供給するため、ストレージ装置と呼ばれる大容量の記憶装置が設けられている。ストレージ装置は、大容量のハードディスクを備えており、各クライアントのユーザは、自己に割り当てられた領域、または共有の領域に対して、データやプログラムなどの格納・読み出しを行う。通常、ストレージ装置へのアクセスには、SCSI (Small Computer System Interface) と呼ばれるプロトコルが使用される。近年では、SCSI用のコマンドを、いわゆるIPパケットに分割してネットワーク上を転送するためのiSCSIと呼ばれるプロトコルが提案されている。iSCSIを用いることにより、従来よりも更に多数のクライアント、および遠隔地のクライアントがストレージ装置にアクセス可能な環境が提供されつつある。10

【0003】

ストレージ装置の活用方法の一つとして、リモートブートと呼ばれるクライアントの起動方法が提案されている。リモートブートでは、起動に必要なオペレーティングシステム、環境設定ファイルなどの各種ファイルが、予めストレージ装置の各ユーザ用の領域に格納されている。各クライアントは、ネットワークを介してこれらのファイルをストレージ装置から読み込むことにより、起動することができる。20

【0004】

リモートブートする場合、クライアントは、ストレージ装置へのアクセスを実現するための比較的小さなブートプログラムをROMに記憶していれば十分であり、ハードディスクを備えている必要がない。ハードディスクに格納されるべきデータはストレージ装置で一元管理されるから、仮にクライアントコンピュータが破損、盗難などに遭っても、重要なデータの遺失、漏洩を逃れることができるというセキュリティ上の利点がある。また、各ユーザは、ネットワーク上に接続されたいずれのクライアントも、一定の環境設定で起動させることができるという実用上の利点もある。リモートブートについては、例えば、特許文献1～3に開示されている。30

【0005】

ストレージ装置を用いる場合、多数のクライアントによるストレージ装置へのアクセスの集中を緩和するため、クライアントとストレージ装置との間に、キャッシング用のメモリを備えたノード装置を設けることがある。かかるシステムでは、ノード装置にキャッシング済みのデータは、ストレージ装置にアクセスするまでなくクライアントに供給可能であるため、ストレージ装置へのアクセスが緩和される。

【0006】

【特許文献1】

特開平6-332716号公報

【特許文献2】

特開2001-75853号公報

【特許文献3】

特開2000-259583号公報

【0007】

【発明が解決しようとする課題】

しかし、ノード装置を用いたシステムでは、このノード装置がセキュリティ上、脆弱になり易いという課題があった。一般に、ストレージ装置は、企業の機密データを一元的に保持しているため、非常に厳しくセキュリティ管理されている。例えば、ストレージ装置が設置された部屋への立ち入りは厳しく制限されており、ソフトウェア的にもファイアウォールなどでストレージ装置へのアクセスは厳しく制限されている。一方、クライアントは4050

、ハードディスクを備えないディスクレスコンピュータとすることにより、データの漏洩を防止することができる。仮に、クライアントがハードディスクを備えている場合でも、各ユーザは、自己が使用する装置については盗難や不正使用に遭わないよう気を配るため、一定レベルでセキュリティは確保される。

【0008】

これに対し、ノード装置に対しては、ストレージ装置ほどセキュリティが確保された環境が確保されておらず、各ユーザもセキュリティに気を配らないことが多い。かかる環境下で、ノード装置には、ストレージ装置とクライアントの間で授受される機密データがキャッシュされている。従って、ノード装置の盗難や不正アクセスによって、機密データが漏洩する可能性があった。かかる機密データの一つとして、例えば、動作に支障が生じた時にクライアントが出力するコアダンプが挙げられる。コアダンプは、通常のコンピュータでは、内蔵のハードディスクに書き出されるが、ディスクレスコンピュータではノード装置にキャッシュされた後、ストレージ装置に書き出される。コアダンプには、ストレージ装置にアクセスするためのパスワードなど、コンピュータに保存されていた種々の機密情報が含まれており、これらの情報の漏洩は、ストレージ装置への不正アクセスを許容する原因となり得る。本発明は、これらの課題に鑑み、ノード装置におけるセキュリティの向上を図ることを目的とする。

10

【0009】

【課題を解決するための手段】

本発明では、ストレージ装置、ノード装置、およびクライアントが接続された計算機システムにおいて、ノード装置に備えられたキャッシュ用のディスク装置へのキャッシュを次の方法で制御する。この制御は、ノード装置の揮発性メモリへのキャッシュにも同様に適用してもよいし、ディスク装置へのキャッシュ時にのみ適用してもよい。

20

【0010】

＜第1の制御方法＞ 第1の制御方法では、ディスク装置へのキャッシュの可否を表す属性情報を用いる。ストレージ装置またはクライアントは、ノード装置によって中継されるデータについて、上述の属性情報をノード装置に対して出力する。ノード装置は、この属性情報に基づいて、キャッシュ否と判断されたデータについては、ディスク装置へのキャッシュを行わずに中継する。こうすることにより、機密データについてはノード装置でのキャッシュを禁止することができ、セキュリティを確保することができる。

30

【0011】

ノード装置がディスク装置の他に、キャッシュ用の揮発性メモリを有している場合、キャッシュ否のデータについては揮発性メモリへのキャッシュを禁止してもよい。また、揮発性メモリに対しては、キャッシュ可否に関わらずキャッシュを行い、揮発性メモリからディスク装置への書き込みは、キャッシュ否と判断されたデータを除いて行うようにしてもよい。

【0012】

キャッシュ可否を制御するための属性情報は、種々のタイミングで取得することができる。例えば、データの中継時に、このデータと関連付けて属性情報を入力するようにしてもよい。ヘッダ等に属性情報を含めることでデータと属性情報を一体として入力してもよいし、中継されるデータと分けて属性情報のみを入力してもよい。かかる態様は、例えば、ストレージ装置において、データごとに属性情報を予め管理しておき、ノード装置に、この属性情報を通知する機能をもたせることにより、実現することができる。

40

【0013】

ストレージ装置において、データの格納ブロックと対応づけて属性情報が管理されている場合、ノード装置は、この対応を予め取得し、管理しておいてもよい。こうすれば、データの中継時にストレージ装置から属性情報を受け取るまでなく、キャッシュの可否を判断することができる。

【0014】

属性情報は、必ずしもデータ単位でキャッシュの可否を通知する情報である必要はない。

50

例えば、クライアントにおけるソフトウェアの動作異常発生を通知する情報を属性情報として用いても良い。ノード装置は、この通知を受信した後は、そのクライアントからのデータのキャッシングを行わないというように、キャッシング可否の動作を切り替えることができる。同様に、クライアントの動作が正常に復帰したことを通知する情報を属性情報として用いても良い。このように、属性情報は、ノード装置におけるキャッシング可否を切り替えるタイミングを通知する情報とすることもできる。

【0015】

かかる通知は、キャッシングの禁止をノード装置に要求するための所定の条件が満たされた時に、ノード装置に対して属性情報を出力する機能をクライアントに持たせることにより実現できる。クライアントは、この属性情報の出力と併せて、または該属性情報の出力後に、データをノード装置に送信するようにすればよい。キャッシングの禁止を要求するための条件は、例えば、上述の動作異常の他、予め設定された特定のアプリケーションの起動時など種々の設定が可能である。

10

【0016】

＜第2の制御方法＞ 本発明の第2の制御方法では、ノード装置において、中継すべきデータを暗号化してディスク装置に書き込むことでキャッシングする。キャッシングされたデータの読み出コマンドを受けた時には、ディスク装置から読み出したデータを復号してストレージ装置またはクライアントに出力する。暗号化は、ディスク装置への書き出し時に完了していればよく、例えば、書き出し直前に行っててもよいし、データの受信時に行っててもよい。こうすることで、ディスク装置が盗難に遭っても、データのセキュリティを確保することができる。

20

【0017】

第2の制御方法においては、必ずしも全てのデータを暗号化する必要はない。例えば、中継するデータについて、暗号化の要否を表す属性情報を入力し、この属性情報に基づいて、暗号化の要否を切り替えても良い。属性情報は、第1の制御方法でキャッシングの可否を制御するために例示した種々の情報を適用することができる。こうすれば、不要な暗号化を抑制することができ、ノード装置での処理負担を軽減することができる。第1の制御方法と同様、属性情報は、暗号化の要否を切り替えるタイミングを通知する情報としてもよい。

30

【0018】

第2の制御方法においては、暗号化および復号に用いる鍵データを揮発性メモリに管理することが好ましい。こうすれば、ノード装置が盗難等にあった場合には、鍵データが消失するため、ディスク装置に記憶されたデータの復号が不能となる。この鍵データは、例えば、ストレージ装置がノード装置に与えるようにしてもよいし、ノード装置自身が生成するようにしてもよい。ストレージ装置から鍵データを供給する場合、ストレージ装置は、各ノード装置に与えられる鍵データに重複が生じないよう管理することが好ましい。こうすることにより、与えられた鍵データは他のノード装置には適用できなくなるため、ノード装置へのなりすましによって鍵データが取得された場合でも、セキュリティを確保することができる。ストレージ装置からノード装置への鍵データの供給は、例えば、ノード装置が新たに稼働し始めた場合や、ノード装置の管理者がストレージ装置に対して鍵データの発行を要求した場合など、種々の条件下で行うことができる。

40

【0019】

＜第3の制御方法＞ 第3の制御方法は、ストレージ装置およびクライアントの一方から他方へのデータ送信時において、データの発信側となるデータ提供装置が、データの送信先を切り換えることにより実現される。データ提供装置は、提供するデータについて、ディスク装置へのキャッシングの可否を判断する。キャッシング可否の判断条件は、例えば、予めデータごとに設定しておいてもよいし、「ソフトウェアの動作異常時」など特定の事象やタイミングとの関係で設定してもよい。データ提供装置はキャッシング可と判断されたデータについては、ノード装置に送信し、ノード装置は、このデータをディスク装置にキャッシングする。キャッシング否と判断されたデータについては、ノード装置を介さずに、受信

50

側の装置に、直接データを送信する。こうすることにより、ノード装置では特別な制御を要することなく、キャッシュを回避することができる。

【0020】

第3の制御方法を実現するため、データ提供装置は、ノード装置とは別に、受信側となる計算機のアドレス情報を予め管理しておいてもよい。データ提供装置は、キャッシュ否と判断された場合には、データの送信先をノード装置のアドレスから、予め管理されているアドレス情報に切り換えることにより、ノード装置を迂回した通信を実現することができる。この様子は、受信側となる計算機のアドレス情報が予め固定されている場合、例えば、クライアントからストレージ装置へのデータ送信時に有用である。

【0021】

別の様子として、ノード装置は、ストレージ装置内のデータの読み出コマンドを受け付けた時、この読み出コマンドを発信したクライアントを特定可能な情報、例えば、アドレス情報、クライアント名、クライアントの識別情報などを、ストレージ装置に送信するようにしてもよい。こうすることでストレージ装置は、ノード装置を迂回する場合のデータの送信先を特定することができる。ストレージ装置が、ノード装置を迂回してクライアントにデータを送信する場合、ノード装置に対して、データの送信が完了した通知を行うようにしてもよい。この通知がノード装置からストレージ装置に出力した読み出コマンドに対する応答となり、ノード装置を応答待ちの状態から解放することができる。

【0022】

本発明は、上述したノード装置、ストレージ装置、クライアントに限らず種々の様子で構成することが可能である。例えば、これらを接続した計算機システムとして構成してもよい。また、ノード装置におけるキャッシュを制御する制御方法として構成してもよい。コンピュータによりこの制御を実現するためのコンピュータプログラムおよびこれを記録した記憶媒体として構成してもよい。ここで、記憶媒体としては、フレキシブルディスクやCD-ROM、DVD、光磁気ディスク、ICカード、ROMカートリッジ、パンチカード、バーコードなどの符号が印刷された印刷物、コンピュータの内部記憶装置（RAMやROMなどのメモリ）および外部記憶装置などコンピュータが読み取り可能な種々の媒体を利用できる。

【0023】

【発明の実施の形態】

本発明の実施の形態について以下の順序で説明する。

A. 第1実施例；

A 1. システム構成；

A 2. 機能ブロック；

A 3. テーブルのデータ構造；

A 4. データ読み出処理；

A 5. データ書き込処理；

A 6. 変形例；

B. 第2実施例；

B 1. 機能ブロック；

B 2. データ読み出処理；

B 3. データ書き込処理；

C. 第3実施例；

C 1. 機能ブロック；

C 2. データ読み出処理；

C 3. データ書き込処理；

【0024】

A. 第1実施例；

A 1. システム構成；

図1は第1実施例としての計算機システムの構成を示す説明図である。この計算機システ 50

ムでは、ストレージ装置300に、複数のノード装置200および計算機100がIPパケットを授受可能なネットワークで接続されている。ネットワークとしては、LAN(Lo cal Area Network)、インターネット、インターネットなどを適用することができる。

【0025】

ストレージ装置300は、図示するハードウェア構成を有するコンピュータとして構成されており、大容量のディスク装置310に蓄積されたデータをノード装置200経由で各計算機100に提供することができる。また、各計算機100はハードディスク310にデータを格納することもできる。NIC(Network Interface Card)304は、ネットワークを介してデータを授受するためのインターフェースである。I/O305は、入出力装置用のインターフェースである。
10

【0026】

ストレージ装置300では、CPU301が、ディスク装置310およびROM303に記憶された制御用のプログラムに従って、データの授受を制御する。メモリ302は、このプログラムの動作時に使用される主記憶である。

【0027】

ノード装置200は、図示するハードウェア構成を有するコンピュータとして構成されており、ストレージ装置300と計算機100の間で授受されるデータを中継する機能を奏する。ディスク装置210およびメモリ202は、中継されるデータを一時的に蓄積するキャッシュのために利用される。NIC(Network Interface Card)204は、ネットワークを介してデータを授受するためのインターフェースである。I/O205は、入出力装置用のインターフェースである。
20

【0028】

ノード装置200では、CPU201が、ディスク装置210およびROM203に記憶された制御用のプログラムに従って、データの中継およびキャッシュを制御する。メモリ202は、キャッシュの他、このプログラムの動作時にも使用される。本実施例では、中継するデータによってキャッシュの可否が切り替えられる。キャッシュが禁止されているデータについては、ノード装置200は、キャッシュを行わずに中継する。キャッシュの禁止については、二通りの制御が適用可能である。第1の態様は、キャッシュが禁止されているデータに関しては、ノード装置200は一切、キャッシュを行わないという制御方法である。第2の態様は、ノード装置200は揮発性のメモリ202には、キャッシュ可否の属性に関わらずキャッシュを行い、メモリ202からディスク装置210にデータを移転する際に、キャッシュの可否を判断する制御方法である。本実施例では、第1の態様でキャッシュの可否を制御するものとして説明し、後で変形例として第2の態様について説明する。
30

【0029】

計算機100は、ハードディスクを備えないディスクレスコンピュータである。内部には、CPU101、RAM102、ROM103、NIC104およびI/O105が備えられている。計算機100は、起動時には、必要なオペレーティングシステムなどのファイルをストレージ装置300から読み込むことで、リモートブートする。ROM103には、リモートブート用のプログラムが予め記憶されている。
40

【0030】

ストレージ装置300、ノード装置200、計算機100の動作を制御するためのプログラムは、CD-ROMなどの記録媒体によってストレージ装置に供給してもよい。

【0031】

A2. 機能ブロック；

図2は計算機システムを構成する各装置内の機能ブロックを示す説明図である。本実施例では、図示する各機能ブロックは、それぞれコンピュータプログラムをインストールすることによりソフトウェア的に構成される。各機能ブロックは、ハードウェア的に構成することも可能である。

【0032】

計算機100の機能ブロックは、次の通りである。TCP/IPモジュール120は、ネットワークを介してIPパケットを通信する。SCSIモジュール122は、ストレージ装置300に対してデータの読み出し、書き込み用のコマンド送受信などを行う。i SCSIモジュール121は、SCSIコマンドとIPパケットの変換を行うことによって、SCSIコマンドをTCP/IPで送受信可能とする。ブートプログラム130は、計算機100でリモートブートを実現する。ブートプログラム130は、計算機100の初期化を行う機能、起動に必要なオペレーティングシステムなどのファイルをストレージ装置から読み込む機能、これらのファイルを起動してブートする機能などを実現することができる。ID入力モジュール131は、リモートブートを行う際に、ストレージ装置300に送信すべきユーザID、パスワードを入力する。本実施例では、これらのモジュールは、ROM103に記憶されているプログラムによって実現される。

10

【0033】

上述の各機能ブロックによってリモートブートが完了すると、計算機100には、ストレージ装置300から供給されたファイルによってオペレーティングシステム140が起動する。オペレーティングシステム140には、計算機100の動作に異常が生じた時に、種々の情報をコアダンプとしてストレージ装置300に書き出す機能を有する異常制御モジュール141が備えられている。計算機100上の各処理に利用されるアプリケーション150は、ストレージ装置300から供給され、オペレーティングシステム140の上で稼働する。

20

【0034】

本実施例では、クライアントごとに仮想ボリュームが与えられる。仮想ボリュームとは、ストレージ装置300のディスク装置310内に設けられた物理的な領域ではなく、各クライアントのデータを管理するための論理的なディスクを意味する。仮想ボリュームは、ユーザIDに対応づけて設定されており、ユーザが、計算機100でユーザIDを入力することによって、計算機100と対応づけられる。以下、本実施例では、「クライアント」という用語は、単にハードウェアとしての計算機ではなく、ユーザがログインし、仮想ボリュームと対応づけられた状態にある計算機を意味するものとする。

【0035】

ノード装置200には、ネットワークを介してSCSIコマンドを授受するため、TCP/IPモジュール220、i SCSIモジュール221、SCSIモジュール222が備えられている。ノード装置200には、所定のオペレーティングシステムがインストールされており、このオペレーティングシステム上で稼働するアプリケーションによってキャッシュ制御モジュール230が実現されている。

30

【0036】

キャッシュ制御モジュール230は、キャッシュ属性管理部234およびキャッシュ管理テーブル232を参照して、ノード装置200におけるキャッシュを制御する。キャッシュ管理テーブル232とは、クライアントから指定された仮想ブロックと、ノード装置200におけるデータの格納場所、即ちキャッシュブロックとを対応づけるテーブルである。キャッシュ属性管理部234とは、仮想ブロックの各データについて、キャッシュの可否を示す属性情報を管理するテーブルである。これらのテーブルのデータ構造については後述する。

40

【0037】

ストレージ装置300には、ネットワークを介してSCSIコマンドを授受するため、TCP/IPモジュール320、i SCSIモジュール321、SCSIモジュール322が備えられている。ストレージ装置300には、所定のオペレーティングシステムがインストールされており、このオペレーティングシステム上で稼働するアプリケーションによってアクセス制御モジュール330が実現されている。

【0038】

アクセス制御モジュール330は、ユーザ管理テーブル334、物理ブロック管理テーブ

50

ル 332 を参照して、ディスク装置 310 のデータの読み書きを制御する。ユーザ管理テーブル 334 は、ユーザ ID と仮想ボリュームとを対応づけるテーブルである。物理ブロック管理テーブル 332 とは、仮想ブロックと物理ブロックとを対応づけるテーブルである。アクセス制御モジュール 330 は、計算機 100 の起動時に、計算機 100 からユーザ ID を取得する。このユーザ ID に基づいてユーザ管理テーブル 334 を参照することで、ユーザに対応する仮想ボリュームを計算機 100 に割り当てる。アクセス制御モジュール 330 は、以後、クライアントから指定された仮想ブロックに対して、物理ブロック管理テーブル 332 を参照して、ディスク装置 310 のデータの読み書きを制御することができる。

【0039】

10

キャッシュ管理テーブル 333 は、仮想ブロックごとにキャッシュの可否を記録したテーブルである。アクセス制御モジュール 330 は、キャッシュ属性管理テーブル 333 の内容をノード装置 200 に通知することで、ノード装置 200 におけるキャッシュの可否を制御する。

【0040】

A 3. テーブルのデータ構造；

図 3 はユーザ管理テーブル 334 の構造を示す説明図である。ユーザ管理テーブル 334 は、ユーザ ID、パスワード、仮想ボリューム、属性、IP アドレスを対応づけて管理する。属性とは、仮想ボリュームに対する他のユーザのアクセスの可否を表している。「専有」は他のユーザのアクセスが禁止されていることを意味し、「共有」は許可されていることを意味する。IP アドレスは、ユーザがログインした計算機によって変動する。属性、IP アドレスは、ユーザ管理テーブル 334 から省略してもよい。

20

【0041】

図 4 は物理ブロック管理テーブル 332 の構造を示す説明図である。図の上方にデータ構造を示し、下方に仮想ブロックと物理ブロックとの対応関係を模式的に示した。物理ブロック管理テーブル 332 は、仮想ブロックと物理ブロックの対応関係を示すテーブルであり、仮想ボリューム単位で設けられている。図中には、仮想ボリューム VD a に対応するテーブルを例示した。このテーブルでは、仮想ボリューム VD a の仮想ブロック BL 0 ~ BL n に対して、実際にデータが格納されている物理ブロックが記憶されている。物理ブロックは、物理ボリュームとブロック番号との組み合わせで定義される。

30

【0042】

図に例示したテーブルは、下方に模式的に示した対応関係を表している。つまり、仮想ブロック BL 0 のデータは、物理ボリューム PD 1 1 のブロック BL 0 に格納されている。同様にして、仮想ブロック BL 1 ~ BL n の各データは、それぞれ物理ボリューム PD 1 1、PD 1 2 のいずれかのブロックに格納されている。図では、ディスク装置 310 が、パーティションによって複数の物理ボリュームに分割されている場合を例示したが、単一の物理ボリュームとして構成されていてもよい。この場合、物理ブロック管理テーブル 332 からは、物理ボリュームに関するデータを省略しても構わない。

【0043】

40

図 5 はキャッシュ管理テーブル 232 の構造を示す説明図である。このテーブルは、仮想ブロックと、ノード装置 200 におけるキャッシュブロックとを対応づけている。ディスク書込の欄については、後述する。ノード装置 200 におけるキャッシュの格納場所には、揮発性のメモリ 202 と、ディスク装置 210 の 2 種類が存在する。従って、本実施例では、格納場所とブロック番号で、キャッシュブロックを特定するものとした。

【0044】

50

図 6 はキャッシュ属性管理テーブル 333 の構造を示す説明図である。キャッシュ属性管理テーブル 333 は、データの読み出しと書き込みに分けて用意されており、仮想ボリュームごとにキャッシュの可否を表す情報を格納している。本実施例では、ディスク装置が複数の物理ボリュームに分割されているため、物理ボリューム単位でキャッシュの可否を設定可能とした。例えば、図の例では、仮想ボリューム VD a の読み出しについて、物理

ボリューム P D 1 1 に格納されたデータについてはキャッシュ可、物理ボリューム P D 1 2 に格納されたデータについてはキャッシュ不可と設定されている。

【0045】

図の例において、物理ボリューム P D 1 2 は、仮想ボリューム V D a 、 V D b に共有されている。本実施例では、このように複数の仮想ボリュームによる物理ボリュームの共有を許容してもよい。この場合、共有される物理ボリュームに格納されたデータは、各仮想ボリュームに対応した複数のクライアントで共有されることになる。図中の例では、共有されている物理ボリューム P D 1 2 について、キャッシュ属性は不可と設定されている場合を例示した。これに対し、仮想ボリューム V D a 、 V D b で、共有されている物理ボリューム P D 1 2 に対するキャッシュ属性を異ならせても良い。こうすることにより、例えば、仮想ボリューム V D a からの読み出し時にはキャッシュを許可し、仮想ボリューム V D b からの読み出し時にはキャッシュを禁止するというように、読み出すクライアントに応じてキャッシュの可否を切り換えることが可能となる。

10

【0046】

書き込みについても、同様の形式でキャッシュの可否が管理されている。キャッシュ可否については、計算機システムの動作時に動的に設定を変更してもよい。例えば、仮想ボリューム V D a を使用するクライアントの動作異常を検知した時、ノード装置 2 0 0 は仮想ボリューム V D a に対応する全物理ボリュームについて、一時的に「キャッシュ不可」の属性を設定するようにしてもよい（図中のデータ領域 D a 参照）。

20

【0047】

A 4. データ読み出処理；

図 7 はデータ読み出処理のフローチャートである。リモートブート時を例にとり、左側にクライアント 1 0 0 の処理、中央にノード装置 2 0 0 の処理、右側にストレージ装置 3 0 0 の処理を示した。

【0048】

ユーザが計算機の電源をオンにすると、 I D 入力モジュール 1 3 1 によって、ユーザ I D 、パスワード等の入力画面が提示される。ユーザが、ユーザ I D 、パスワードを入力し、ログインすると、クライアント 1 0 0 は、 I P アドレスとともにこれらの情報を、ノード装置 2 0 0 およびストレージ装置 3 0 0 に送信する（ステップ S 1 0）。ストレージ装置 3 0 0 は、この情報に基づいてユーザ管理テーブル 3 3 4 を参照し、ユーザの認証を行う（ステップ S 3 0）。正規なユーザであることが確認されると、ストレージ装置 3 0 0 は、ユーザ管理テーブル 3 3 4 に、クライアント 1 0 0 の I P アドレスを記録するとともに、ユーザに対応した仮想ボリューム名を通知する。この通知は、ノード装置 2 0 0 を介してクライアント 1 0 0 に送信される。以後、クライアント 1 0 0 からのデータの読み出しが要請される場合は、この仮想ボリューム名に基づいて行われる。

30

【0049】

クライアント 1 0 0 は、 R O M に記録されているブートプログラム 1 3 0 を起動する（ステップ S 1 1）。ブートプログラム 1 3 0 は、ブートに必要な初期化処理を行った上で、オペレーティングシステムのデータ読み出しが要請される（ノード装置 2 0 0 に対して送信する（ステップ S 1 2）。

40

【0050】

ノード装置 2 0 0 は、読み出しが要請されたデータを受信し、キャッシュ管理テーブル 2 3 2 を参照して、要求されたデータが、既にキャッシュ済みであるか否かを確認する（ステップ S 2 0）。キャッシュ済みの場合は（ステップ S 2 0）、キャッシュブロックから該当するデータを読み出し（ステップ S 2 6）、クライアント 1 0 0 に返信する（ステップ S 2 5）。クライアント 1 0 0 は、このデータを受信して起動処理を継続する（ステップ S 1 3）。

【0051】

要求されたデータがキャッシュされていない（以下、「未キャッシュ」と呼ぶ）場合（ステップ S 2 0）、ノード装置 2 0 0 はストレージ装置 3 0 0 にデータの読み出しが要請される（ステップ S 2 1）。ストレージ装置 3 0 0 は、この要求に応じて、物理ブロック管理

50

テーブル 332 を参照して、物理ボリュームからデータを読み出し、ノード装置 200 に返信する（ステップ S32）。これと併せて、ストレージ装置 300 は、キャッシング属性管理テーブル 333 を参照し、要求されたデータのキャッシング可否の属性情報をノード装置 200 に通知する（ステップ S32）。この属性情報は、要求されたデータのヘッダ等に埋め込んだ形で通知してもよいし、要求されたデータと分けて通知してもよい。

【0052】

ノード装置 200 は、ストレージ装置 300 からデータおよび属性情報を受信すると、属性情報に基づいてキャッシングの可否を判断する（ステップ S22）。キャッシング可と判断される場合には、受信したデータをキャッシングし（ステップ S23）、その格納先に応じてキャッシング管理テーブル 232 を更新して（ステップ S24）、データをクライアントに返信する（ステップ S25）。キャッシング不可と判断される場合には、上述のキャッシング処理をスキップし、データをクライアントに返信する（ステップ S25）。クライアントはこうしてノード装置 200 から送信されたデータを受信する（ステップ S13）。

10

【0053】

以上の処理を繰り返し行うことにより、クライアント 100 は、ブートに必要なファイルを取得し、リモートブートを完了することができる。図 7 ではリモートブート時の読み出し処理を示したが、リモートブートと無関係に通常のデータ読み出し時にも、データ読み出し要求（ステップ S12）からデータ受信（ステップ S13）の処理が同様にして行われる。

20

【0054】

上述の実施例では、データの要求時にノード装置 200 からストレージ装置 300 にキャッシングの可否を問い合わせる場合を例示した。これに対し、ノード装置 200 は、ストレージ装置 300 から、予めキャッシング属性管理テーブル 333 の内容をまとめて取得し、キャッシング属性管理部 234 で管理するようにもよい。こうすることにより、データ要求のたびに、属性情報の問い合わせを行う必要性をなくすことができる。

【0055】

A5. データ書き込み処理；

図 8 はデータ書き込み処理のフローチャートである。左側にクライアント 100 の処理、中央にノード装置 200 の処理、右側にストレージ装置 300 の処理を示した。クライアント 100 は既に起動し、ノード装置 200 、ストレージ装置 300 とデータ授受が可能な状態で、クライアント 100 の動作にソフトウェア上の異常が生じた場合のコアダンプの書き込みを例示した。

30

【0056】

クライアント 100 の異常制御モジュール 141 は、ソフトウェア上の動作異常を検出すると（ステップ S40）、異常の発生を IP アドレスとともにノード装置 200 に通知する（ステップ S40）。ノード装置 200 は、この情報に基づいてキャッシング属性管理部 234 における属性情報を更新する（ステップ S50）。先に図 6 で示したように、このクライアントからの書き込みについては、全てキャッシング不可という属性に変更するのである。

40

【0057】

クライアント 100 の異常制御モジュール 141 は、仮想ブロックを指定して、コアダンプを書き込むための要求をノード装置に送信する（ステップ S42）。ノード装置 200 は、書き込み要求を受信し、キャッシング属性管理部 234 を参照して、キャッシングの可否を判断する（ステップ S52）。クライアント 100 の動作に異常が生じた場合には、ノード装置 200 は、ステップ S50 で更新された属性情報に基づき、キャッシング不可と判断することになる。一方、クライアント 100 に異常が生じる前、異常から回復した後、および別のクライアントからの書き込み要求時などには、指定された仮想ブロックの属性情報に基づき、ノード装置 200 はキャッシング可と判断する場合もある。

【0058】

キャッシング可と判断した場合（ステップ S52）、ノード装置は、クライアントから受信

50

したデータをキャッシングし（ステップS53）、その格納先に応じてキャッシング管理テーブル232を更新するとともに（ステップS54）、データをストレージ装置300に送信する（ステップS55）。キャッシング不可と判断した場合（ステップS52）、ノード装置200は、クライアントから受信したデータをキャッシングすることなく、ストレージ装置300に送信する（ステップS55）。ストレージ装置は、ノード装置200からデータを受信して（ステップS60）、指定された仮想ブロックに書き込みを行う。

【0059】

以上の処理を繰り返し行うことにより、クライアント100は、ストレージ装置300の仮想ブロックにデータの書き込みを行うことができる。この際、異常が生じた場合のコアダンプについては、ノード装置へのキャッシングを回避することができる。

10

【0060】

上述の実施例では、クライアント100の異常通知により、ノード装置200がキャッシング可否の属性情報を更新する場合を例示した。これに対し、クライアント100からノード装置200に送信されるデータごとにキャッシング可否の属性情報を添付するようにしてもよい。例えば、異常制御モジュール141は、コアダンプとして書き込むデータについては、全てキャッシング不可という属性情報を添付し、ノード装置200は、この属性情報に基づいてキャッシングの可否を判断するようにしてよい。

【0061】

A6. 変形例；

実施例では、ストレージ装置300からのデータ読み込み時、およびストレージ装置300への書き込み処理時にノード装置200が一切、キャッシングを行わない例を示した。ノード装置200は、キャッシング可否に関わらず、揮発性メモリ202へのキャッシングを行い、メモリ202からディスク装置210へのデータ移転時にキャッシングの可否を判定するようにしてもよい。かかる制御は、ディスク装置210への書き込み時に、キャッシング属性管理部234とキャッシング管理テーブル232を参照することで実現することができる。つまり、キャッシング管理テーブル232を参照することにより、メモリ202にキャッシングされているデータについて、仮想ボリュームおよびブロック番号を特定することができる。この情報に基づいて、キャッシング属性管理部234を参照すれば、ディスク装置210へのキャッシング可否を判定することができる。

20

【0062】

変形例の制御を実現するための別の方法として、キャッシング管理テーブル232に、図5の破線で示した「ディスク書込」という情報を設けても良い。「ディスク書込」は、ディスク装置210へのキャッシング可否を表す属性情報であり、メモリ202へのキャッシング時に、キャッシング属性管理部234を参照することで設定することができる。このようにキャッシング管理テーブル232において、格納されているデータごとに、ディスク書込を保存しておくことにより、ディスク装置210への移転時にキャッシング属性管理部234を参照する必要がなくなり、キャッシング可否を簡易に判定することができる。

30

【0063】

以上で説明した第1実施例によれば、データの読みだし、および書き込み時に、ノード装置200におけるディスク装置210へのキャッシングの可否を切り替えることができる。コアダンプなど、機密情報を含むデータについては、ディスク装置210へのキャッシングを回避することができるため、ノード装置200の盗難による情報漏洩を抑止することができる。ノード装置200においてメモリ202へのキャッシング自体も禁止する場合には、ノード装置200への不正アクセスによる情報漏洩を抑止することも可能である。

40

【0064】

B. 第2実施例；

第1実施例では、属性情報に基づいて、ノード装置200におけるキャッシング可否を切り替える例を示した。第2実施例では、ノード装置が、ディスク装置へのキャッシング時に、データを暗号化することでセキュリティを確保する例を示す。ノード装置への不正アクセスに対するセキュリティ確保という観点からは、メモリ202へのキャッシング時にもデー

50

タを暗号化してもよい。ただし、本実施例においては、暗号化に要する処理負荷を軽減するため、メモリ202へのキャッシング時には暗号化を行わず、ディスク装置210へのデータ移転時に暗号化する例を示す。

【0065】

B 1. 機能ブロック；

図9は第2実施例としての計算機システムの機能ブロックを示す説明図である。第1実施例と同じ機能ブロックについては、同一の符号で示した。第2実施例では、キャッシング属性管理部234、キャッシング属性管理テーブル333に確保されている属性情報は、キャッシングの可否ではなく、暗号化の要否を示す情報となる。第2実施例では、ノード装置200Aに暗号化部235が新たに追加され、ストレージ装置300Aに鍵管理モジュール335が新たに追加される。暗号化部235は、ノード装置200Aにおいて、ディスク装置210へのキャッシング時に、データの暗号化を行う機能、およびディスク装置210から読み出されたデータを復号する機能を奏する。鍵管理モジュール335は、ノード装置200Aに対して、暗号化に使用する鍵情報を管理・提供する機能を奏する。

10

【0066】

B 2. データ読出処理；

図10は第2実施例におけるデータ読出処理のフローチャートである。左側にクライアント100の処理、中央にノード装置200Aの処理、右側にストレージ装置300Aの処理を示した。第2実施例では、ノード装置200Aがネットワークに接続され、起動すると、ストレージ装置300Aは、ノード装置200Aに対して鍵情報の送信を行う（ステップS31）。ノード装置200Aは、この鍵情報を暗号化部235に記憶する（ステップS70）。

20

【0067】

本実施例においては、鍵情報は、ノード装置ごとに固有の情報として設定される。ストレージ装置300は、ネットワークに接続されている複数のノード装置について、提供した鍵情報を一元的に管理し、新たに接続されたノード装置に対しては、これらのいずれとも異なる鍵情報を生成する。鍵情報は、例えば、シリアル番号などの規則的なものであってもよいし、乱数を用いた不規則な情報であってもよい。各ノード装置に一意な鍵情報を提供することにより、いわゆる悪意の第三者がノード装置になりすまして鍵情報を取得した場合でも、各ノード装置にキャッシングされたデータのセキュリティを確保することができる利点がある。

30

【0068】

クライアント100がノード装置200Aに対して、データの読みだし要求を送信すると（ステップS12）、ノード装置200Aは、要求されたデータが、キャッシング済みであるか否かを判断する（ステップS71）。キャッシング済みである場合には、メモリ202またはディスク装置210からデータを読みだし（ステップS72）、暗号化されている場合には、復号して（ステップS73、S74）、クライアント100に返信する（ステップS81、ステップS13）。

【0069】

要求されたデータがキャッシングされていない場合（ステップS71）、ノード装置200Aは、ストレージ装置300Aにデータを要求する（ステップS75）。ストレージ装置300Aは、この要求に応じて、データをノード装置200Aに返信する（ステップS32）。これと併せて、ストレージ装置300は、要求されたデータについて暗号化の要否を表す属性情報をノード装置200Aに通知する（ステップS32）。この属性情報は、要求されたデータのヘッダ等に埋め込んだ形で通知してもよいし、要求されたデータと分けて通知してもよい。

40

【0070】

ノード装置200Aは、ストレージ装置300Aからデータおよび属性情報を受信すると、データのキャッシング先を判断する（ステップS76）。メモリ202にキャッシング可能な領域があいている場合には、メモリ202へのキャッシングを行う。キャッシング可能な領

50

域が空いていない場合には、ディスク装置 210 へのキャッシュが必要と判断する。この判断は、ストレージ装置 300A からのデータ受信時に行つても良いし、いわゆる LRU (Least Recently Used) に基づいて処理してもよい。LRU とは、メモリ 202 にキャッシュされているデータのうち、アクセス頻度の低いデータを優先的にディスク装置 210 に移転する方法である。LRU で処理する場合には、ストレージ装置 300A から受信したデータは、無条件にメモリ 202 にキャッシュされ、代わりに、従前にメモリ 202 に蓄積されていたデータのいずれかがディスク装置 210 に移転されることになる。

【0071】

ノード装置 200A は、ディスク装置 210 にキャッシュすべきと判断されたデータについては（ステップ S76）、属性情報に基づいて暗号化の要否を判断する（ステップ S77）。暗号化が要求されている場合には、暗号化を行い（ステップ S78）、キャッシュする（ステップ S79）。暗号化が要求されていないデータ、またはメモリ 202 にキャッシュすべきデータについては（ステップ S76）、暗号化を行わずにキャッシュする。ノード装置 200A は、これらのキャッシュの格納先に応じて、キャッシュ管理テーブル 232 を更新し（ステップ S80）、データをクライアント 100 に返信する（ステップ S25）。クライアントはこうしてノード装置 200 から送信されたデータを受信する（ステップ S13）。

【0072】

以上の処理を繰り返し行うことにより、クライアント 100 は、必要なファイルをストレージ装置 300A から読み出すことができる。この際、機密情報を含むデータについては、属性情報の設定により、ディスク装置 210 へのキャッシュ時に暗号化することができるため、セキュリティを確保することができる。第 2 実施例においても第 1 実施例と同様、ノード装置 200A が、暗号要否の属性情報をストレージ装置 300A から、予めまとめて取得し、管理するようにしてもよい。

【0073】

B3. データ書込処理；

図 11 は第 2 実施例におけるデータ書込処理のフローチャートである。左側にクライアント 100 の処理、中央にノード装置 200A の処理、右側にストレージ装置 300A の処理を、コアダンプの書き込みを例にとって示した。

【0074】

読みだし処理と同じく、ノード装置 200A は起動時に、ストレージ装置から鍵情報を受信し、記憶している（ステップ S60、S31）。また、第 1 実施例と同様、クライアント 100 の異常制御モジュール 141 は、ソフトウェア上の動作異常を検出すると（ステップ S40）、異常の発生を IP アドレスとともにノード装置 200 に通知する（ステップ S40）。ノード装置 200 は、この情報に基づいてキャッシュ属性管理部 234 における属性情報を暗号化要という内容に更新する（ステップ S50）。

【0075】

この状態で、クライアント 100 がコアダンプを書き込むための要求をノード装置 200A に送信すると（ステップ S42）、ノード装置 200A は、読みだし処理と同様、受信したデータのキャッシュ先を判断する。ノード装置 200A は、ディスク装置 210 にキャッシュすべきと判断されたデータについて、属性情報で指定された暗号化の要否に基づいて暗号化を行った上で、キャッシュする（ステップ S90～S93）。暗号化が要求されていないデータ、またはメモリ 202 にキャッシュすべきデータについては（ステップ S90）、暗号化を行わずにキャッシュする（ステップ S94）。ノード装置 200A は、これらのキャッシュの格納先に応じて、キャッシュ管理テーブル 232 を更新し（ステップ S94）、データをストレージ装置 300A に送信する（ステップ S95）。ストレージ装置 300A は、ノード装置 200A からデータを受信して（ステップ S60）、指定された仮想ブロックに書き込みを行う。以上の処理を繰り返し行うことにより、クライアント 100 は、ストレージ装置 300A の仮想ブロックにデータの書き込みを行うこと

10

20

30

40

50

ができる。

【0076】

第2実施例によれば、ノード装置200Aにおいて、ディスク装置への書き込み時に暗号化することにより、盗難によるデータの漏洩を抑止することができる。メモリ202への書き込み時には暗号化を行わないため、頻繁に使用されるデータについては、メモリ202にキャッシングしておくことにより、読みだし、書き込みの速度を確保することもできる。

【0077】

第2実施例では、鍵情報をストレージ装置300Aから提供したが、鍵情報は厳密に一意である必要はなく、ノード装置200Aで生成しても構わない。第2実施例では、属性情報によって暗号化の要否を制御する場合を例示したが、ディスク装置210へのキャッシング時には必ず暗号化するようにしてもよい。

10

【0078】

C. 第3実施例：

第3実施例では、キャッシング可とされているデータについては、クライアントとストレージ装置間でノード装置を介してデータの授受を行い、キャッシング不可とされているデータについては、両者間で直接データの授受を行う場合を例示する。

【0079】

C 1. 機能ブロック；

図12は第3実施例としての計算機システムの機能ブロックを示す説明図である。第1実施例と同じ機能ブロックについては、同一の符号で示した。第3実施例では、クライアント100に提供されるオペレーティングシステム140Bの内容が、第1実施例と相違する。オペレーティングシステム140Bは、SCSIコマンドの送出先としてノード装置200Bのアドレス（以下、「ノードアドレス」と称する）142を保持している。オペレーティングシステム140Bには、動作異常時にコアダンプの書き込みなどを行う異常制御モジュール141Bが供えられており、この異常制御モジュール141Bは、コアダンプの書き込み先としてストレージ装置300Bのアドレス（以下、「ストレージアドレス」と称する）143を保持している。これらの機能ブロックにより、クライアントは、異常時と正常時でデータの書き込み先を切り替えることができる。

20

【0080】

ストレージ装置300Bにおいては、アクセス制御モジュール330Bが、キャッシング属性に基づいてデータの送信先を切り替える。キャッシング可とされているデータについてはノード装置に送信し、キャッシング不可とされているデータはクライアント100に直接送信する。第3実施例では、キャッシング不可とされているデータについては、クライアント100とストレージ装置300Bの間で直接送受信されるから、ノード装置200Bにおいて、キャッシング制御モジュール230Bは、クライアント100およびストレージ装置300Bから受信したデータについては、キャッシング可否を考慮することなく、データをキャッシングする。

30

【0081】

C 2. データ読み出し処理；

図13は第3実施例におけるデータ読み出し処理のフローチャートである。リモートポート時を例にとり、左側にクライアント100の処理、中央にノード装置200Bの処理、右側にストレージ装置300Bの処理を示した。

40

【0082】

ユーザが計算機の電源をオンにすると、第1実施例と同様の手順でログインおよびブートプログラムの起動が行われる（ステップS10、S30、S11）。クライアント100は、仮想ボリュームを指定して、データの読み出し要求をノード装置200Bに対して送信する（ステップS12）。

【0083】

ノード装置200Bは、要求されたデータがキャッシング済みの場合は（ステップS100 50

)、キャッシュブロックから該当するデータを読み出し（ステップS101）、クライアント100に返信する（ステップS105）。クライアント100は、このデータを受信して起動処理を継続する（ステップS13）。

【0084】

要求されたデータが未キャッシュの場合（ステップS100）、ノード装置200Bはストレージ装置300Bにデータの読み出しを要求する（ステップS102）。ストレージ装置300Bは、キャッシュ属性管理テーブル333において、要求されたデータがキャッシュ可と設定されている場合には（ステップS110）、データをノード装置に返信する（ステップS111）。ノード装置200Bは、このデータをキャッシュし（ステップS103）、キャッシュ管理テーブル232を更新して（ステップS24）、データをクライアントに返信する（ステップS105）。 10

【0085】

要求されたデータがキャッシュ不可の場合には（ステップS110）、ストレージ装置300Bは、データをクライアントに直接、返信する（ステップS112）。クライアントはこうしてノード装置200から送信されたデータを受信する（ステップS13）。ストレージ装置300Bは、ノード装置200Bに対して、クライアントへの返信を行った旨の通知を行っても良い。ノード装置200Bが、データの要求（ステップS102）へのレスポンスを待っている場合には、この通知により、レスポンス待ちの状態から解放することができる。 20

【0086】

上記実施例において、ストレージ装置300Bからクライアントに直接、データを送信する場合、クライアントのアドレスは種々の方法で特定することができる。例えば、ストレージ装置300Bは、最初のログイン時にユーザ管理テーブル334に記録されているIPアドレスを利用してもよい。別の例として、データの要求時に、ノード装置200Bからストレージ装置300Bに対して、クライアント100のアドレス情報を通知するようにしてよい。 30

【0087】

C.3. データ書き込み処理；

図14はデータ書き込み処理のフローチャートである。左側にクライアント100の処理、中央にノード装置200Bの処理、右側にストレージ装置300Bの処理を、コアダンプの書き込みを例にとって示した。クライアント100は、異常が生じていない場合には（ステップS120）、ノード装置200に対してデータの書き込み要求を送信する（ステップS121）。ノード装置200Bは、この要求を受信すると、データをキャッシュし（ステップS13）、キャッシュ管理テーブル232を更新する（ステップS131）。その後、キャッシュされている書き込みデータが所定量に達したなど、予め設定されたタイミングで、データをストレージ装置300Bに送信する（ステップS132）。ストレージ装置300Bは、このデータを受信して、指定された仮想ブロックにデータの書き込みを行う（ステップS140）。 30

【0088】

一方、異常制御モジュール141が、ソフトウェア上の動作異常を検出すると（ステップS120）、データの送信先をノード装置200のアドレスからストレージ装置に切り替えることにより、ストレージ装置300Bに対して直接、データの書き込み要求を送信する（ステップS122）。ストレージ装置300Bは、このデータを受信して、指定された仮想ブロックにデータの書き込みを行う（ステップS140）。 40

【0089】

第3実施例によれば、キャッシュの可否によって、ノード装置200Bを迂回してデータを送受信することができる。従って、ノード装置の盗難や不正アクセスに対し、データのセキュリティを確保することができる。

【0090】

以上、本発明の種々の実施例について説明したが、本発明はこれらの実施例に限定されず 50

、その趣旨を逸脱しない範囲で種々の構成を探ることができることはいうまでもない。

【0091】

【発明の効果】

本発明によれば、ノード装置へのキャッシング自体の回避、キャッシング時の暗号化、ノード装置を迂回したデータ授受などの方法により、機密情報を含んだデータ等がノード装置のディスク装置に、原状でキャッシングされることを回避することができる。従って、ノード装置の盗難、不正アクセスに対して、これらのデータのセキュリティを確保することができる。

【図面の簡単な説明】

- 【図1】第1実施例としての計算機システムの構成を示す説明図である。 10
- 【図2】計算機システムを構成する各装置内の機能ブロックを示す説明図である。
- 【図3】ユーザ管理テーブル334の構造を示す説明図である。
- 【図4】物理ブロック管理テーブル332の構造を示す説明図である。
- 【図5】キャッシング管理テーブル232の構造を示す説明図である。
- 【図6】キャッシング属性管理テーブル333の構造を示す説明図である。
- 【図7】データ読み出し処理のフローチャートである。
- 【図8】データ書き込み処理のフローチャートである。
- 【図9】第2実施例としての計算機システムの機能ブロックを示す説明図である。
- 【図10】第2実施例におけるデータ読み出し処理のフローチャートである。
- 【図11】第2実施例におけるデータ書き込み処理のフローチャートである。 20
- 【図12】第3実施例としての計算機システムの機能ブロックを示す説明図である。
- 【図13】第3実施例におけるデータ読み出し処理のフローチャートである。
- 【図14】データ書き込み処理のフローチャートである。

【符号の説明】

- 100…クライアント
- 101、201、301…CPU
- 102、202、302…メモリ(RAM)
- 103、203、303…ROM
- 104、204、304…NIC
- 105、205、305…I/O
- 120、220、320…TCP/IPモジュール
- 121、221、321…iSCSIモジュール
- 122、222、322…SCSIモジュール
- 130…ブートプログラム
- 131…ID入力モジュール
- 140、140B…オペレーティングシステム
- 141、141B…異常制御モジュール
- 142…ノードアドレス
- 143…ストレージアドレス
- 150…アプリケーション
- 200、200A、200B…ノード装置
- 210、310…ディスク装置
- 230、230B…キャッシング制御モジュール
- 232…キャッシング管理テーブル
- 234…キャッシング属性管理部
- 235…暗号化部
- 300、300A、300B…ストレージ装置
- 330、330B…アクセス制御モジュール
- 332…物理ブロック管理テーブル
- 333…キャッシング属性管理テーブル

10

20

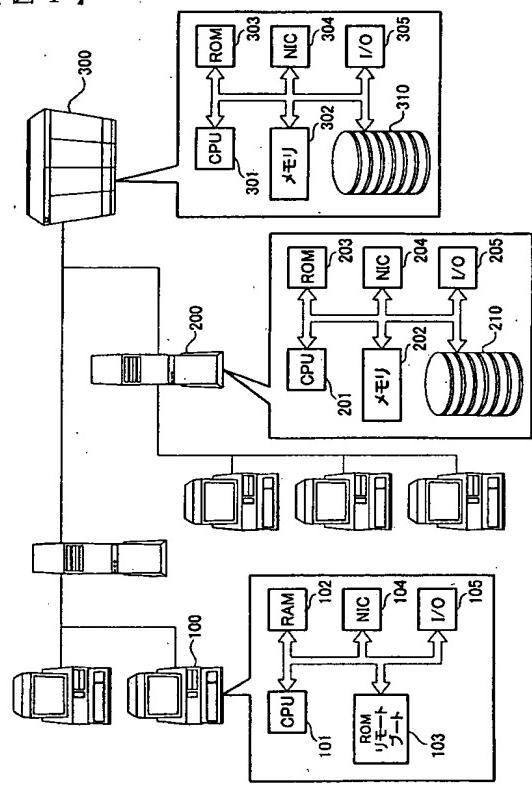
30

40

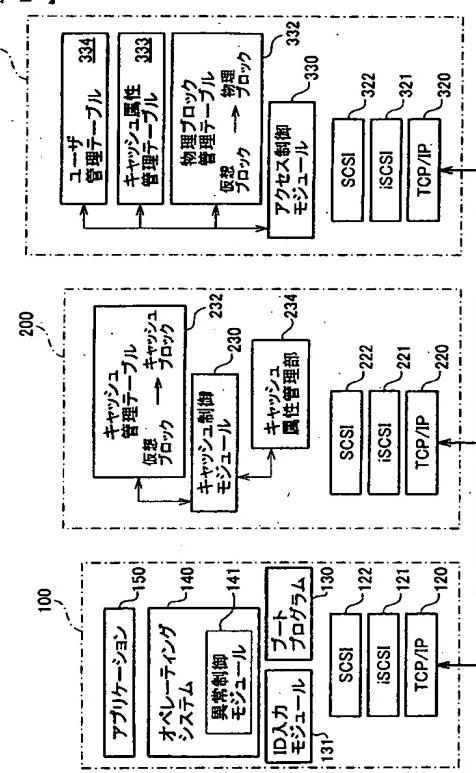
50

3 3 4 … ユーザ管理テーブル

【図 1】



【図 2】



【図3】

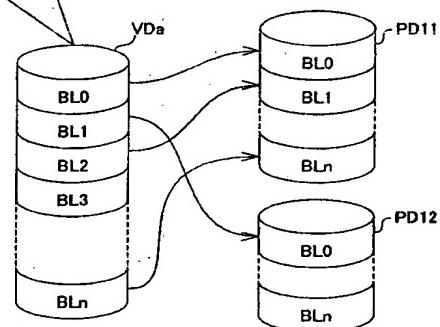
334

	ユーザ名	パスワード	仮想ボリューム	属性	IPアドレス
	ユーザA	*****	VDA	専有	IPa
	ユーザB	*****	VDB	専有	
	ユーザC	*****	VDO	共有	

【図4】

332

仮想ブロック	物理ブロック	
	物理ボリューム	ブロック
VDa	PD11	BL0
VDa	PD12	BL0



【図5】

232

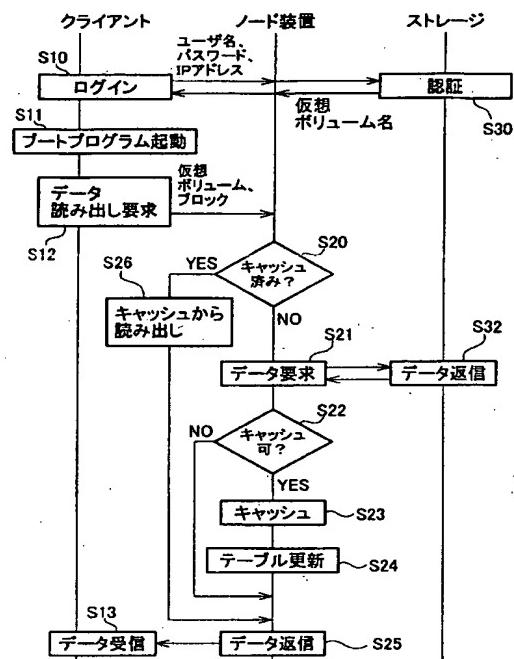
仮想ブロック	プロック	キャッシュブロック	ディスク書き込み
VDa	BL0	ディスク	BL0 可
VDb	BL0	メモリ	BL1 可
VDa	BL1	メモリ	BL0 不可
VDb	BL2	ディスク	BL3 可

【図6】

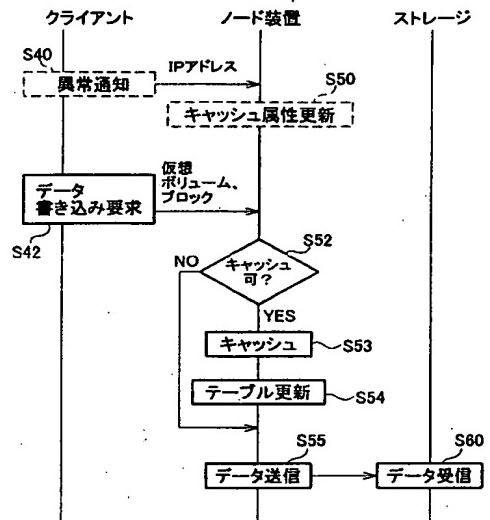
234

仮想ボリューム	読み出し		書き込み	
	物理ボリューム	キャッシュ	物理ボリューム	キャッシュ
VDA	PD11	可	PD11'	不可
	PD12	不可	PD12	不可
VDb	PD21	可	PD21	可
	PD12	不可	PD12	不可

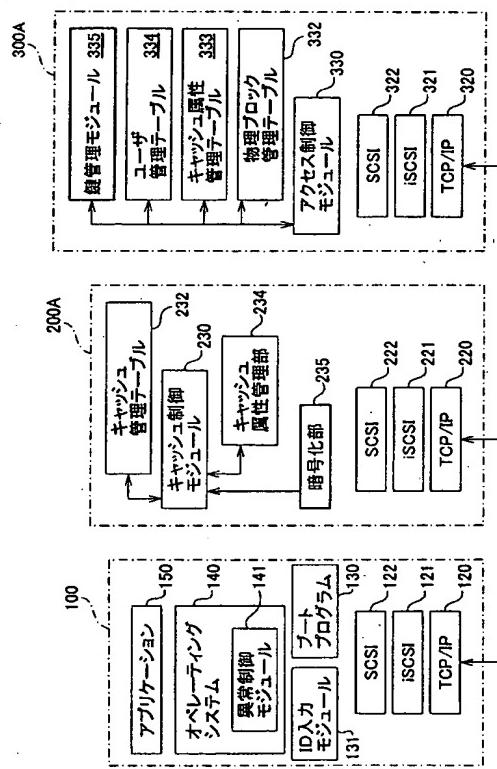
【図7】



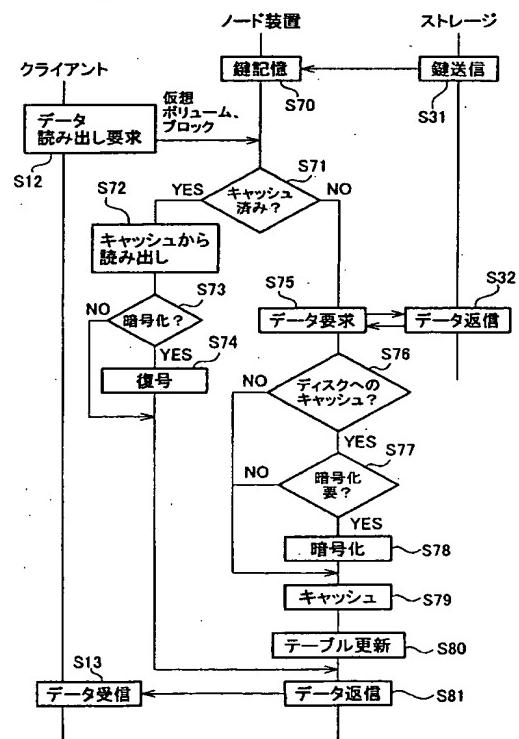
【図8】



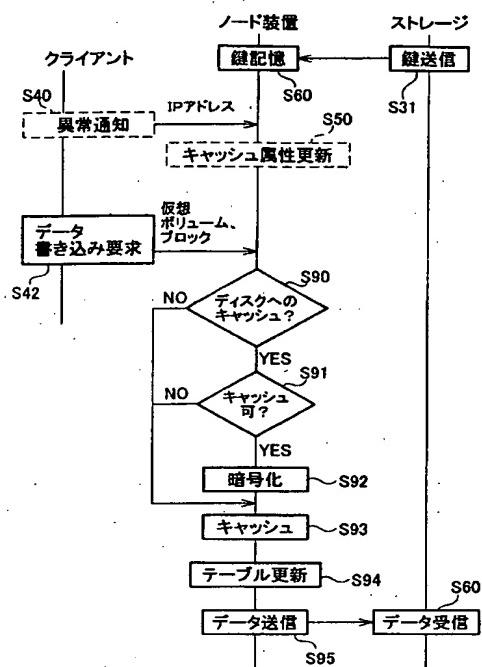
【図9】



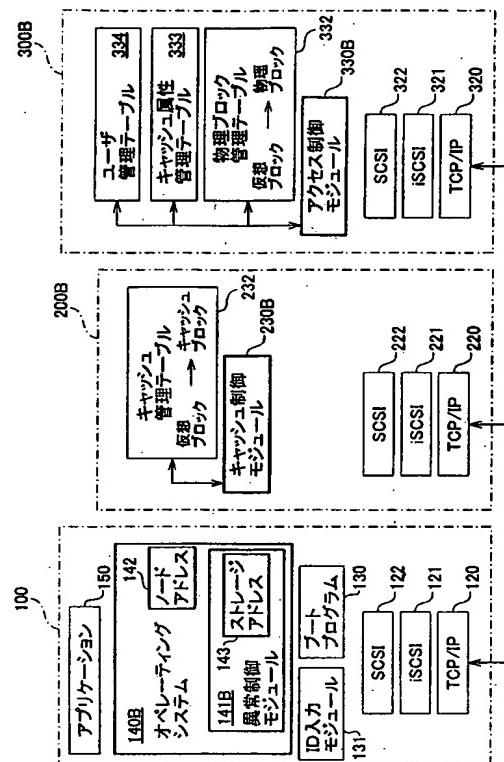
【図10】



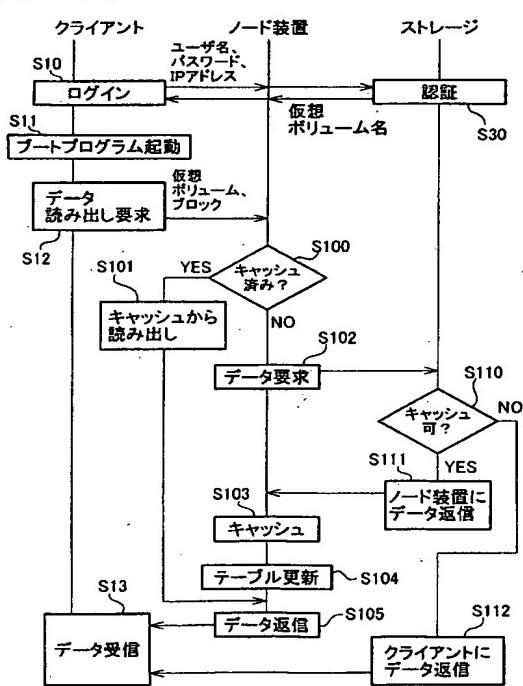
【図1-1】



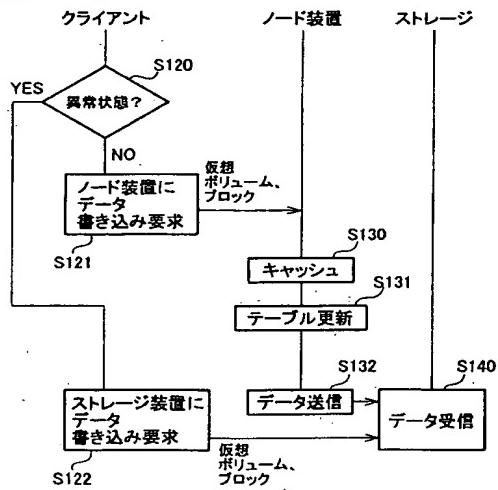
【図1-2】



【図1-3】



【図1-4】



フロントページの続き

(72)発明者 橋本 尚

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内
Fターム(参考) 5B082 GA11 HA02